CLAIMS

1. The method for mutual authentication of a first station and a second station, comprising:

encrypting a particular data random key at the first station by first veiling the particular data random key using a first conversion array seeded by a shared secret and then encrypting the veiled particular data random key to produce a first encrypted key, where access to the shared secret indicates authenticity of the first station;

sending a first message to the second station including the first encrypted key, where the second station decrypts and unveils said particular data random key using the shared secret, and where the second station encrypts the particular data random key by first veiling a version of the particular data random key using a second conversion array seeded by the shared secret and then encrypting the veiled version of the particular data random key to produce a second encrypted key, and sends a second message to the first station carrying the second encrypted key, where access to the shared secret indicates authenticity of the second station; and

receiving the second message, and decrypting and unveiling the version of the particular data random key at the first station.

2. The method of claim 1, including

encrypting an additional particular data random key at the first station by first veiling the additional particular data random key using a first conversion array seeded by an additional shared secret and then encrypting the veiled particular data random key to produce a first additional encrypted key, where access to the additional shared secret indicates authenticity of the first station;

sending a third message to the second station including the additional encrypted key, where the second station decrypts and unveils said additional particular data random key using the additional shared secret, and where the second station encrypts the additional particular data random key by first veiling a version of the additional particular data random key using a second conversion array seeded by the additional shared secret and then encrypting the veiled version of the additional particular data random key to

produce a second additional encrypted key, and sends a second message to the first station carrying the second additional encrypted key, where access to the additional shared secret indicates authenticity of the second station; and

receiving the second message, and decrypting and unveiling the version of the additional particular data random key at the first station.

3. The method of claim 2, wherein said additional particular data random key is the same as the particular data random key.

4. The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

5. The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

placing a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

6. The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

7. The method of claim 1, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

8. The method of claim 1, including presenting a use interface to the second station from the first station carrying parameters of said first and second conversion arrays.

9. The method of claim 1, including executing an interactive exchange of messages to deliver the particular data random key from the first station to the second station.

10. A data processing apparatus, comprising:

a processor, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to encrypt a particular data random key at the first station by first veiling the particular data random key using a first conversion array seeded by a shared secret and then encrypting the veiled particular data random key to produce a first encrypted key, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted key, where the second station decrypts and unveils said particular data random key using the shared secret, and where the second station encrypts the particular data random key by first veiling a version of the particular data random key using a second conversion array seeded by the shared secret and then encrypting the veiled version of the particular data random key to produce a second encrypted key, and sends a second message to the first station carrying the second encrypted key, where access to the shared secret indicates authenticity of the second station; and

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station.

11. The apparatus of claim 10, including logic to encrypt an additional particular data random key at the first station by first veiling the additional particular data random key using a first conversion array seeded by an additional shared secret and then encrypting the veiled particular data random key to produce a first additional encrypted key, where access to the additional shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the additional encrypted key, where the second station decrypts and unveils said additional particular data random key using the additional shared secret, and where the second station encrypts the additional particular data random key by first veiling a version of the additional particular data random key using a second conversion array seeded by the additional shared secret and then encrypting the veiled version of the additional particular data random key to produce a second additional encrypted key, and sends a second message to the first station carrying the second additional encrypted key, where access to the additional shared secret indicates authenticity of the second station; and

logic to receive the second message, and to decrypt and unveil the version of the additional particular data random key at the first station.

12. The apparatus of claim 11, wherein said additional particular data random key is the same as the particular data random key.

13. The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

14. The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X

values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

to place a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

15. The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

16. The apparatus of claim 10, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

17. The apparatus of claim 10, including logic to present a user interface to the second station from the first station carrying parameters of said first and second conversion arrays.

18. The apparatus of claim 10, including logic to execute an interactive exchange of messages to deliver the particular data random key from the first station to the second station.

19. An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising

logic to encrypt a particular data random key at the first station by first veiling the particular data random key using a first conversion array seeded by a shared secret and then encrypting the veiled particular data random key to produce a first encrypted key, where access to the shared secret indicates authenticity of the first station;

logic to send a first message to the second station including the first encrypted key, where the second station decrypts and unveils said particular data random key using the shared secret, and where the second station encrypts the particular data random key by first veiling a version of the particular data random key using a second conversion array seeded by the shared secret and then encrypting the veiled version of the particular data random key to produce a second encrypted key, and sends a second message to the

first station carrying the second encrypted key, where access to the shared secret indicates authenticity of the second station; and

logic to receive the second message, and to decrypt and unveil the version of the particular data random key at the first station.

20. The article of claim 19, the instructions including logic to encrypt an additional particular data random key at the first station by first veiling the additional particular data random key using a first conversion array seeded by an additional shared secret and then encrypting the veiled particular data random key to produce a first additional encrypted key, where access to the additional shared secret indicates authenticity of the first station;

logic to send a third message to the second station including the additional encrypted key, where the second station decrypts and unveils said additional particular data random key using the additional shared secret, and where the second station encrypts the additional particular data random key by first veiling a version of the additional particular data random key using a second conversion array seeded by the additional shared secret and then encrypting the veiled version of the additional particular data random key to produce a second additional encrypted key, and sends a second message to the first station carrying the second additional encrypted key, where access to the additional shared secret indicates authenticity of the second station; and

logic to receive the second message, and to decrypt and unveil the version of the additional particular data random key at the first station.

21. The article of claim 19, wherein said additional particular data random key is the same as the particular data random key.

22. The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X

values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

to place a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

23. The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

to place a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

24. The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

25. The article of claim 19, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and the instructions include logic to

generate one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

use a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

place a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

map the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

26. The article of claim 19, wherein the instructions include logic to present a user interface to the second station from the first station carrying parameters of said first and second conversion arrays.

27. The article of claim 19, wherein the instructions include logic to execute an interactive exchange of messages to deliver the particular data random key from the first station to the second station.